(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年5 月19 日 (19.05.2005)

PCT

(10) 国際公開番号
WO 2005/045789 A1

(51) 国際特許分類[7]: G09C 1/00, G06F 9/30

(21) 国際出願番号: PCT/JP2004/016589

(22) 国際出願日: 2004 年11 月9 日 (09.11.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2003-380114
2003 年11 月10 日 (10.11.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 独立行政法人科学技術振興機構 (JAPAN SCIENCE AND TECHNOLOGY AGENCY) [JP/JP]; 〒3320012 埼玉県川口市本町四丁目１番８号 Saitama (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 曽我正和 (SOGA, Masakazu) [JP/JP]; 〒0200045 岩手県盛岡市盛岡駅西通１−２−１−８０２ Iwate (JP). 猪股俊光 (INOMATA, Toshimitsu) [JP/JP]; 〒0200887 岩手県盛岡市上ノ橋町５−５−２０１ Iwate (JP).

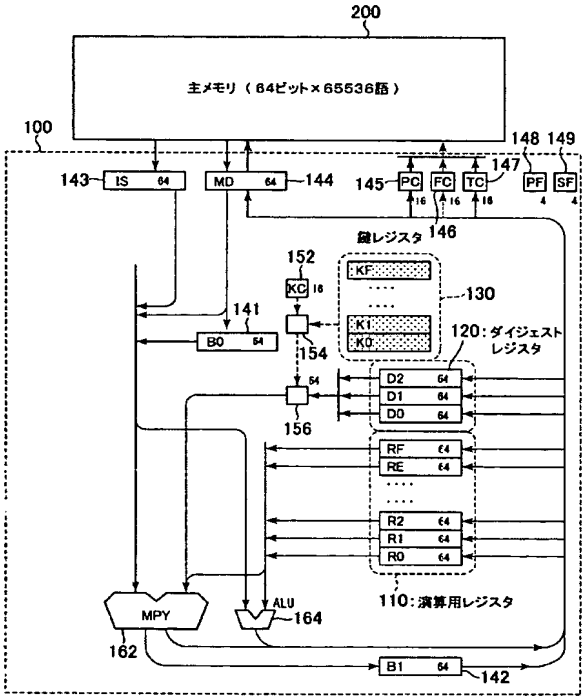
(74) 代理人: 加古進 (KAKO, Susumu); 〒1700013 東京都豊島区東池袋三丁目１番４号 メゾンサンシャイン９０２ Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: SECURE PROCESSOR

(54) 発明の名称: セキュア・プロセッサ



200... MAIN MEMORY (64 BITS × 65536 WORDS)
130... KEY REGISTER
120... DIGEST REGISTER
110... OPERATION REGISTER

(57) Abstract: There is provided a processor having the general purpose function as well as the security function (i.e., safe storage of key data and high-speed calculation of a digital signature). In the secure processor (100) having a general purpose instruction and a signature calculation instruction, a non-volatile key register (130) contains key data. A key bit reference counter (152) is successively decremented from 1023 to 0. According to the content of the key bit reference counter (152), K data stored in the key register (130) is successively specified by one bit from a bit specification gate (154) so as to be successively used for calculation of a signature. There is provided no word data parallel transmission route for transmitting data from the key register (130) containing the key K to another unit. With this hardware structure, it is impossible to output the key data as raw data directly outside.

(57) 要約: 汎用機能を持ち、なおかつ、セキュリティ機能（すなわち鍵データの安全保管とディジタル署名計算の高速化）も持つプロセッサの提供。 一般用と署名演算用の命令を有するセキュア・プロセッサ１００内に、不揮発性の鍵レジスタ１３０に、鍵データが格納されている。鍵ビット参照カウンタ１５２は１０２３から０まで、順次デクリメントする。この鍵ビット参照カウンタ１５２の内容により、ビット指定ゲート１５４から、鍵レジスタ１３０に格納されているＫデータが順次１ビットづつ指定され、逐次署名演算に使用される。鍵Ｋを格納する鍵レジスタ１３０から他へデータを転送する語データ並列伝送経路を設けていない。 このようなハードウェア構造からして、鍵データを生の形で直接外部へ出すことは不可能である。

WO 2005/045789 A1

SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。